

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP TP. HCM**  
**KHOA CÔNG NGHỆ THÔNG TIN**

-----🙞🙜🕮🙞🙜-----

**ĐỒ ÁN 1**

**XÂY DỰNG HỆ THỐNG IPS**

**DÙNG HIDS-OSSEC**



GVHD: Nguyễn Hoà

Sinh viên thực hiện:  
1. Phạm Văn Duẩn (13037321)

2. Võ Thành Luân()

3. Mai Quốc Qui (13032721)

4. …Vinh ()

*TP. Hồ Chí Minh, tháng 5 năm 201**6*

1. **Đặt vấn đề**
   1. **Tầm quan trọng của IDS**
   2. **Vai trò của HIDS**
   3. **Bài toán đặt ra của đề tài**
2. **Mô hình hệ thống và phương pháp thực hiện**
   1. **Mô hình hệ thống**
   2. **Công nghệ thực hiện**
   3. **Phương pháp thực hiện**
3. **Các module phân tích và xử lý log của đề tài**
   1. **Nhận dạng log**
   2. **Lấy log từ workstation**
   3. **Decode log**
      1. **Predecode**

Quá trình predecode chỉ để trích xuất các thông tin đơn giản của event. Predecode thường được sử dụng với các log message có định dạng được sử dụng phổ biến như syslog.

Các thông tin được trích xuất qua giai đoạn này bao gồm:

* **hostname:** nơi tạo ra log
* **program\_name:** chương trình tạo ra log
* **log:** nội dung chính của log

Ta xét một ví dụ đơn giản về ssh:

Log message: “Oct 28 14:21:39 atropo sshd[855]: Accepted password for piopio from 192.168.3.13 port 45018 ssh2”

Và đây là kết quả từ OSSEC-Logtest

\*\*Phase 1: Completed pre-decoding.

full event: 'Oct 28 14:21:39 atropo sshd[855]: Accepted password for piopio from 192.168.3.13 port 45018 ssh2'

hostname: 'atropo'

program\_name: 'sshd'

log: 'Accepted password for piopio from 192.168.3.13 port 45018 ssh2'

Ta có thể thấy là chỉ có các thông tin cơ bản được trích xuất. Ngoài ra các thông tin như: người dùng, process id, status, source ip,… thì lại không được hiển thị. Vậy nên cần phải thông qua một tiến trình nữa để có thể lấy được các thông tin này, đó chính là decode.

Có một vấn đề nữa ở predecode là đối với những định dạng log khác thì predecode sẽ không thể trích xuất được thông tin mà phải chuyển thẳng đến quá trình decode.

* + 1. **Decode**

Decode là tiến trình diễn ra ngay sau khi predecode. Mục đích của decode là trích xuất các thông tin từ log để có sử dụng trong rule ngay sau khi decode diễn ra. Các thông tin này chính là thông tin về: người dùng, ip source, process id, status,… và các thông tin cần thiết khác.

Các option của decoder

* **program\_name:** thực thi decode nếu program\_name của log phù hợp với program\_name được cấu hình
* **prematch:** thực thi decode nếu tìm thấy trong file log có thành phần khớp với prematch
* **regex:** dùng biểu thức regular expression để xác định các thành phần cần trích xuất
* **offset:** là thuộc tính của regex. Có thể là after\_prematch hoặc after\_parent. ở đây được cấu hình là các biểu thức regular expression.
* **order:** đặt tên cho các dữ liệu được lấy ra từ regex.
* **parent:** được dùng trong cấu hình hàm con của một decoder.

Dưới đây là các field dùng để gán cho từng dữ liệu trích được từ file log:

* **Location:** nơi sinh log
* **srcuser:** source user
* **dstuser:** destination user
* **srcip:** source ip
* **dstip:** destination ip
* **srcport:** source port
* **dstport:** destnation port
* **protocol:** tên giao thức
* **id:** event id
* **url:** địa chỉ
* **status:** trạng thái
* **extra-data:** dữ liệu

Ta có ví dụ về log message được sinh ra sau khi tạo chia sẽ folder trên windows:

WinEvtLog: Security: AUDIT\_SUCCESS(5140): Microsoft-Windows-Security-Auditing: (no user): no domain: VanDuan-PC: A network share object was accessed. Subject: Security ID: S-1-5-21-739373341-442988835-2982865765-1000 Account Name: VanDuan Account Domain: VANDUAN-PC Logon ID: 0x24EF400 Network Information: Object Type: File Source Address: fe80::9d4d:93cc:9f6d:c594 Source Port: 12922 Share Information: Share Name: \\\*\123 Share Path: \??\C:\WINDOWS\System32 Access Request Information: Access Mask: 0x1 Accesses: ReadData (or ListDirectory)

Ta thử trích xuất các thông tin được tô màu bên trên với decoder được viết như sau:

<decoder name=*"windows-file-share-create"*>

<prematch>\.(5140)\.</prematch>

</decoder>

<decoder name=*"windows-file-share-create-sub"*>

<parent>windows-file-share-create</parent>

<regex>^\.+:\.+: (\.+)\((\d+)\): </regex>

<regex>\.+Account Name:\s\s(\w+)\s\s\sAccount Domain:\s\s(\w+)\s\s\s</regex>

<order>status, id, user, extra\_data</order>

</decoder>

<decoder name=*"windows-file-share-create-sub"*>

<parent>windows-file-share-create</parent>

<regex>\.+Share Path:\s\s\\\p+\\(\.+)\s\s\s</regex>

<order>url</order>

</decoder>

Kết quả có được:

\*\*Phase 2: Completed decoding.

decoder: 'windows-file-share-create'

status: 'AUDIT\_SUCCESS'

id: '5140'

dstuser: 'VanDuan'

extra\_data: 'VANDUAN-PC'

url: 'C:\WINDOWS\System32'

Có thể thấy được, ta dễ dàng có được các thông tin cần thiết để so khớp với rule thông qua decoder nhờ sử dụng các biểu thức regular expression.

* 1. **Rule**
  2. **Alert và Active Reponse**

1. **Kết quả thực hiện**
   1. **Kết quả đạt được**
   2. **Hạn chế**
2. **Hướng phát triển**